are from victims who feel as though law enforcement just doesn't care about their plight in these particular cases. The victims believe either the officer does not consider identity theft important enough to spend time on or doesn't believe the consumer is really a victim.

Those beliefs are just a by-product of the many challenges facing law enforcement in investigating these cases. When it comes to identity theft investigations, it is not that law enforcement officers don't care about the victim's plight, but a true lack of manpower, overload of cases, lack of resources and lack of identity theft-specific training all can prohibit many agencies from offering these victims the support they desperately crave.

For victims of identity theft, no matter how big or small the loss, once the crime has been discovered, they are scared and desperate for quick answers.

"Your identity being stolen is like you've been violated — it's almost like being robbed or assaulted," Farris said. "People are going through your personal things, so it almost feels like a physical assault."

Since identity theft can be a repetitive crime, some victims may display symptoms associated with repeated physical assault. It feels like it will never end, especially when they keep receiving more notices by phone or in the mail from creditors, the ITRC notes. Many victims report that the financial, emotional and criminal assault on their good name takes years to recover from and has permanently impacted their lives.

WHERE TO BEGIN

That's why knowing how to work these cases and where to begin unraveling the crime is crucial for detectives today. Effective communication between law enforcement and the victim can be the difference between secondary wounding or a cooperative victim who helps the case go forward.

"When someone realizes they are a victim of identity theft, we need to stop the bleeding as quickly as possible," Farris said.

Hopkinsville Detective Scott Raup agrees.

"The quicker the victim knows about it, the quicker we find out about it and the easier it is for us to follow up on leads," he said. >>

File It: NCIC Identity Theft File

For years, law enforcement officers have been able to enter data on stolen vehicles, firearms and property into the National Crime Information Center files. For officers, these files are invaluable in recovering stolen property. But in 2005, the NCIC Identity Theft File was created as a means to flag stolen identities and help officers recognize imposters when they encounter them in various situations.

When victims learn they have had their identity stolen and they file a police report, the local law enforcement agency taking the report can use the victim's information to create a victim profile for the Identity Theft File, such as name, date of birth and social security number, to name a few. The victim then selects a password that can easily be recalled and is stored with the victim profile.

Since the NCIC file is available to law enforcement nationwide, when an officer encounters an individual during a routine traffic stop, for instance, a query into the NCIC system automatically searches the Identity Theft File as well. If the query matches information of an identity theft victim, the officer will receive the victim profile and the password. If the individual they have stopped does not know the password when asked, the officer may have the imposter, and not the victim.

"It is not an opportunity to arrest, but an opportunity to investigate further," said Detective John Mellen with the Louisville Police Department's Financial Crimes Unit.

Having the information available can help tremendously in piecing together identity theft investigations that can often span several states and become difficult and convoluted.

There are a couple of conditions that must be met in order to have a profile entered in the FBI's Identity Theft File. First, each request must be supported by an official complaint record by a law enforcement agency. Secondly, documentation for the identity theft complaint must meet the following criteria before an entry can be made into the Identity Theft File:

1. Someone is using a means of identification belonging to the victim.
2. The identity of the victim is being used without the victim's permission.
3. The victim's identity is being used or intended to be used to commit an unlawful activity.
4. The victim must sign a waiver prior to the information being entered into the Identity Theft File. ■